Optimizing Cyber Security by Implementing Markov Decision Processes

Andrew Min and Daron Prater – Advisor: Dr. Theodore Allen, Ph.D.

Department of Integrated Systems Engineering

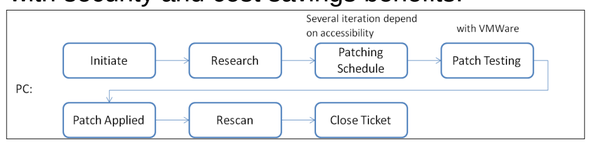
The Ohio State University

The Ohio State University College of Engineering

INTRODUCTION

Background – The amount of sensitive data within organizations continues to grow exponentially. This data is being shared between billions of hosts on laptops, smartphones, and much more. Cyber criminals are aware of potential vulnerabilities on these hosts and are driven by a wide range of motives from financial gain to terrorism. However, preventing against cyber attacks can come at a steep cost. There are many aspects of cyber security and this research focuses on the vulnerability maintenance aspect.

Importance – 90+% of cyber intrusions exploit known vulnerabilities on a host. Currently, many organizations implement simple and often "toothless" policies where risks are usually accepted when patches are not available. Constructing a firm policy that targets and eliminates dangerous vulnerabilities and monitors low impact vulnerabilities provides organizations with security and cost savings benefits.



Previous Work – Hou (2015), Afful-Dadzie (2012), and Allen (2014) have all explored methods for creating optimal cyber security policies. Yet, the previous methods made unrealistic cost assumptions and were based on methods that were potentially to complicated to seem transparent to officials. This research adopts metrics from Hou (2015) and imputation methods from Afful-Dadzie (2012).

GOALS

1. Create a improved cyber maintenance policy for the College of Engineering to potentially save hundreds of thousands of dollars annually.
2. Document more realistic cost assumptions and decision options than previous work.
3. Complete a successful case study of our policy and document any savings.

METHODS

Process –

1. *Data Extraction:* Retrieved and formatted 22 months of Nessus scan data provided by The Ohio State University. Roughly over 2 million vulnerabilities were analyzed.
2. *Data Imputation:* Afful-Dadzie (2012) explored mean based data imputation which was used in this research to replace missing values.
3. *Counts & Transitions:* Hou (2015) used R-code to tabulate transition tables. This research utilized Microsoft Excel VBA to cleanse the data and then tabulate the transition tables.
4. *Policy Generation: W*e use the probabilities of the counts and transitions to create an optimal actions policy for the 12 operating systems via value iteration.

Expected Cost Minimization (Standard MDP):

$$\underbrace{V^*(Y_1,\mathbf{p},\mathbf{r},\gamma)}_{\text{Optimal Objective Value}} = \min_{\mathbf{x}_1,\ldots,\mathbf{x}_{H-1}} \underbrace{V(\mathbf{x}_1,\ldots,\mathbf{x}_{H-1},Y_1,\mathbf{p},\mathbf{r},\gamma)}_{\text{Value for a Given Policy}}$$

$$\text{subject to: } V(\mathbf{x}_1,\ldots,\mathbf{x}_{H-1},Y_1,\mathbf{p},\mathbf{r},\gamma) = E_{Y_1,Y_2,\ldots,Y_H}\Big[\sum_{t=1}^{H-1}\gamma^{t-1} r^{a_t|\mathbf{x}_t}_{Y_t,Y_{t+1},\theta_t} + \gamma^{H-1} r^0_{Y_H}\Big].$$

$$Y_t|Y_{t-1},a_{t-1},\mathbf{p}^{a_{t-1}} \sim Multinomial[Row_{Y_{t-1}}(\mathbf{p}^{a_{t-1}})].$$

Where:

$Y_1 = Current\ natural\ state$

$p = A\ tensor\ of\ all\ transition\ matrices\ for\ all\ action$

$r = Reward$

$\gamma = Discount\ factor$

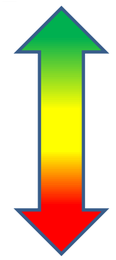
$x = Given\ policy$

Policy Generation Using Value Iteration:

$$V_t^*(i) = \min_a\Big[\sum_{j=1}^{N} p^a_{i,j}(r^a_{i,j,\theta} + \gamma V^*_{t-1}(j))\Big]\ \forall i = 1,\ldots,N$$

Severity Risk Levels –

S1 = Low
S2 = Medium
S3 = High
S4 = Critical
S5 = Compromised



Actions –

1. Do Nothing – Allow the host to operate with no intervention (possibly auto patch is on).
2. Research Accept – Hou (2015) indicates manual reviewing has been conducted on the host and vulnerability will be fixed if there is a solution available. If not, the vulnerability will be placed on risk accepted list, potentially waiting multiple months before elimination.
3. Research Reject – Upgrading needs an average 10 labor hours of work with a 100% chance of eliminating the top two levels.
4. Remediation – Host is placed on firewalled list and banned from network access.

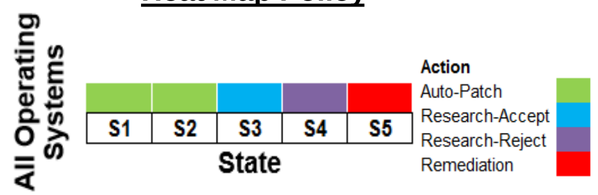
RESULTS

Counts and Transitions Table
Research Accept

From→To	S1	S2	S3	S4	S5
S1	0%	0%	0%	0%	0%
S2	1.8%	87.5%	1.8%	5.4%	3.6%
S3	3.4%	48.0%	48.0%	0.2%	0.4%
S4	2.3%	13.5%	0.4%	81.5%	2.3%
S5	15.8%	42.1%	2.6%	36.8%	2.6%

Cost Assumptions – Mr. Jim Guliani assisted in the development of the cost assumptions. Assumptions were based on average time spent for a human to find a patch for a vulnerability. Ms. Helen Patton provided key access and insights.

Heat Map Policy



1. Introduced two new actions
   a. Research Reject – Upgrading
   b. Remediation
2. More accurate cost assumptions
   a. Based on first-hand knowledge of costs

CONCLUSIONS

1. An optimal policy can be derived from evaluating vulnerabilities on hosts and tracking them over time
2. Implementing this policy based off of known probabilities can lead to an estimated $170,000 in cost savings

FUTURE WORK

- Break down the Nessus data by individual operating systems
- Re-evaluate metrics for defining the severity risk level of a host
- Case study of policy with College of Engineering

REFERENCES

1. Afful-Dadzie, A. and T. T. Allen (in press), "Control Charting Methods for Autocorrelated Cyber Vulnerability Data," Quality Engineering.
2. Afful-Dadzie, A. and T. T. Allen (2014), "Data-Driven Cyber Vulnerability Maintenance Policies," Journal of Quality Technology, 26 (3), 1-17.
3. Chengjun Hou (2015), "Dynamic Programming for Parametric Uncertainty with Applications in Project Management and Cyber Security."
4. Afful-Dadzie, Anthony (2012), "Robust Optimal Maintenance Policies and Charts for Cyber Vulnerability Management.

ACKNOWLEDGEMENTS

We would like to thank Dr. Theodore Allen for his endless support this semester with our cyber security research. We would also like to thank Mr. Jim Giuliani for his knowledge and assistance.